## REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks.

Claims 1-40 are pending in the application, with claims 1, 18, and 31 being independent. Claims 1, 18 and 31 are amended herein. Support for the claim amendments and additions can be found in the original disclosure at least in paragraphs [0043]-[0051]. No new matter has been added.

### § 103 Rejections

**Claims 1-10, 13-25, 28-37, and 40** stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 5724427 (Reeds) in view of U.S. Patent No. 6646639 (Greene), and further in view of U.S. Patent No. 7230978 (Bitterlich).

Applicant respectfully traverses the rejection. Nevertheless, without conceding the propriety of the rejection and in the interest of expediting allowance of the application, claims 1, 18 and 31 has been amended as proposed during the interview and is believed to be allowable.

**Independent claim 1**, as presently presented recites, among other things, "sequentially storing <u>pointers to </u>a plurality of results provided by a stream cipher output rule in a first, second, and third storage units," "wherein the pairing function is $p(x, y) = x \oplus (ay + b)$, where $a$ and $b$ are two constants, and $a$ is odd or $p(x, y) = \gamma, \delta$ is chosen as a nearly universal hash function by the iteration of the following rules:

$$\alpha = ax \bmod 2^{2n}$$

$$\beta = by \bmod 2^{2n}$$

$$\gamma = \alpha^L + \beta^R \bmod 2^{2n}$$

$$\delta = \alpha^R + \beta^L \bmod 2^{2n},$$

where $x^L$ and $x^R$ respectively denote the left and right halves of $x$, and $a,b$ are chosen randomly," and "serially and recursively rotating contents of the first, second, and third storage units, wherein the contents of the storage units are the pointers."

Reeds is directed to a particular method and apparatus for encrypting text using an autokeyed rotational state vector (Reeds, Abstract), and was cited for its alleged teaching of "sequentially storing a plurality of results provided by a stream cipher" (Office Action, page 2). Reeds discloses "an autokeyed rotational state vector may be used to vary the relationship between the alphabets in the cipher during the encryption process." (Reeds, col. 4, lines 9-13.) However, Reeds fails to disclose or suggest at least the elements described above and as presently recited in independent claim 1. This is not surprising, since Reeds is not concerned with "providing a plurality of results from a pairing function" "wherein the pairing function is $p(x,y) = x \oplus (ay + b)$, where $a$ and $b$ are two constants, and $a$ is odd or $p(x,y) = \gamma,\delta$ is chosen as a nearly universal hash function."

Greene is directed to a method for avoiding reading z-values in a graphics pipeline (Greene, col. 5, lines 1-3) and was cited for its alleged teaching of "using the threshold value to determine whether to perform an arithmetic operation." Office Action, page 3. However, Greene fails to remedy the deficiencies in Reeds noted above with respect to claim 1. For example, Greene fails to disclose or suggest at least the elements described above and as presently recited in claim 1.

Bitterlich is directed to a reconfigurable channel CODEC processor for a wireless communication system (Bitterlich, col. 1, lines 45-48) and was cited for its alleged teaching of an output buffer. Office Action, page 3. However, Bitterlich fails to remedy the deficiencies in Greene or Reeds noted above with respect to claim 1. For example, Bitterlich fails to disclose or suggest at least the elements described above and as presently recited in claim 1.

Thus, Reeds, Greene, and Bitterlich whether taken alone or in combination (assuming for the sake of argument that they can be combined), fail to disclose or suggest the features of claim 1. Accordingly, as discussed during the interview, independent claim 1 is allowable.

**Dependent claims 2-8 and 13-17** depend from independent claim 1 and are allowable by virtue of this dependency, as well as for additional features that they recite.

**Independent claim 18**, as presently presented recites, among other things, "sequentially storing pointers to a plurality of results provided by a stream cipher output rule in a first, second, and third portion of the system memory," "wherein the pairing function is $p(x,y) = x \oplus (ay+b)$, where $a$ and $b$ are two constants, and $a$ is odd or $p(x,y) = \gamma, \delta$ is chosen as a nearly universal hash function by the iteration of the following rules:

$$\alpha = ax \bmod 2^{2n}$$

$$\beta = by \bmod 2^{2n}$$

$$\gamma = \alpha^{L} + \beta^{R} \bmod 2^{2n}$$

$$\delta = \alpha^R + \beta^L \bmod 2^{2n},$$

where $x^L$ and $x^R$ respectively denote the left and right halves of $x$, and $a,b$ are chosen randomly," and "serially and recursively rotating contents of the first, second, and third portions of the system memory, wherein the contents of the system memory are the pointers."

Reeds is directed to a particular method and apparatus for encrypting text using an autokeyed rotational state vector (Reeds, Abstract), and was cited for its alleged teaching of "sequentially storing a plurality of results provided by a stream cipher" (Office Action, page 2). Reeds discloses "an autokeyed rotational state vector may be used to vary the relationship between the alphabets in the cipher during the encryption process." (Reeds, col. 4, lines 9-13.) However, Reeds fails to disclose or suggest at least the elements described above and as presently recited in independent claim 18. This is not surprising, since Reeds is not concerned with "providing a plurality of results from a pairing function" "wherein the pairing function is $p(x,y) = x \oplus (ay+b)$, where $a$ and $b$ are two constants, and $a$ is odd or $p(x,y) = \gamma, \delta$ is chosen as a nearly universal hash function."

Greene is directed to a method for avoiding reading z-values in a graphics pipeline (Greene, col. 5, lines 1-3) and was cited for its alleged teaching of "using the threshold value to determine whether to perform an arithmetic operation." Office Action, page 3. However, Greene fails to remedy the deficiencies in Reeds noted above with respect to claim 18. For example, Greene fails to disclose or suggest at least the elements described above and as presently recited in claim 18.

Bitterlich is directed to a reconfigurable channel CODEC processor for a wireless communication system (Bitterlich, col. 1, lines 45-48) and was cited for its alleged teaching of an output buffer. Office Action, page 3. However, Bitterlich fails to remedy the deficiencies in Greene or Reeds noted above with respect to claim 18. For example, Bitterlich fails to disclose or suggest at least the elements described above and as presently recited in claim 18.

Thus, Reeds, Greene, and Bitterlich whether taken alone or in combination (assuming for the sake of argument that they can be combined), fail to disclose or suggest the features of claim 18. Accordingly, as discussed during the interview, independent claim 18 is allowable.

**Dependent claims 19-25 and 28-30** depend from independent claim 18 and are allowable by virtue of this dependency, as well as for additional features that they recite.

**Independent claim 31**, as presently presented recites, among other things, "sequentially storing pointers to a plurality of results provided by the stream cipher in a first, second, and third storage units," "wherein the pairing function is $p(x,y) = x \oplus (ay + b)$, where *a* and *b* are two constants, and *a* is odd or $p(x,y) = \gamma, \delta$ is chosen as a nearly universal hash function by the iteration of the following rules:

$$\alpha = ax \bmod 2^{2n}$$

$$\beta = by \bmod 2^{2n}$$

$$\gamma = \alpha^L + \beta^R \bmod 2^{2n}$$

$$\delta = \alpha^R + \beta^L \bmod 2^{2n},$$

where $x^L$ and $x^R$ respectively denote the left and right halves of *x*, and *a,b* are chosen randomly," and "serially and recursively rotating contents of the first, second, and third storage units, thereby strengthening the cipher stream, wherein the contents of the storage units are the pointers."

Reeds is directed to a particular method and apparatus for encrypting text using an autokeyed rotational state vector (Reeds, Abstract), and was cited for its alleged teaching of "sequentially storing a plurality of results provided by a stream cipher" (Office Action, page 2). However, Reeds fails to disclose or suggest at least the elements described above and as presently recited in independent claim 31.

Greene was cited for its alleged teaching of "using the threshold value to determine whether to perform an arithmetic operation." Office Action, page 3. However, Greene fails to remedy the deficiencies in Reeds noted above with respect to claim 31. For example, Greene fails to disclose or suggest at least the elements described above and as presently recited in claim 31.

Bitterlich was cited for its alleged teaching of an output buffer. Office Action, page 3. However, Bitterlich fails to remedy the deficiencies in Greene or Reeds noted above with respect to claim 31. For example, Bitterlich fails to disclose or suggest at least the elements described above and as presently recited in claim 31.

Thus, Reeds, Greene, and Bitterlich whether taken alone or in combination (assuming for the sake of argument that they can be combined), fail to disclose or suggest the features of claim 31. Accordingly, as discussed during the interview, independent claim 31 is allowable.

**Dependent claims 32-37 and 40** depend from independent claim 31 and are allowable by virtue of this dependency, as well as for additional features that they recite.

**Claims 11-12, 26-27, and 38-39** stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 5724427 (Reeds) in view of U.S. Patent No. 6646639 (Greene), and further in view of U.S. Patent No. 7230978 (Bitterlich), and further in view of U.S. Patent No. 7170997 (Petersen).

Applicant respectfully traverses the rejection. Nevertheless, without conceding the propriety of the rejection and in the interest of expediting allowance of the application, claims 1, 18 and 31 from which the above claims depend have been amended as proposed during the interview and are believed to be allowable. As discussed above, Reeds, Greene, and Bitterlich lack features of independent claims 1, 18, and 31. Therefore, Reeds, Greene, and Bitterlich lack features of dependent claims 11-12, 26-27, and 38-39, at least by virtue of their dependence from their respective base claims.

Peterson was cited for its alleged teaching of a random walk. Office Action, page 6. However, Peterson fails to remedy the deficiencies in Reeds, Greene, or Bitterlich noted above with respect to claim 1. For example, Peterson fails to disclose or suggest "sequentially storing pointers to a plurality of results provided by a stream cipher output rule in a first, second, and third storage units," "wherein the pairing function is $p(x,y) = x \oplus (ay+b)$, where $a$ and $b$ are two constants, and $a$ is odd or $p(x,y) = \gamma, \delta$ is chosen as a nearly universal hash function by the iteration of the following rules:

$$\alpha = ax \bmod 2^{2n}$$

$$\beta = by \bmod 2^{2n}$$

$$\gamma = \alpha^{L} + \beta^{R} \bmod 2^{2n}$$

$$\delta = \alpha^{R} + \beta^{L} \bmod 2^{2n},$$

where $x^L$ and $x^R$ respectively denote the left and right halves of $x$, and $a,b$ are chosen randomly," and "serially and recursively rotating contents of the first, second, and third storage units, wherein the contents of the storage units are the pointers," as presently recited in claim 1.

Thus, Reeds, Greene, Bitterlich, and Peterson, whether taken alone or in combination (assuming for the sake of argument that they can be combined), fail to disclose or suggest the features of claim 1. Accordingly, as discussed during the interview, independent claim 1 is allowable.

**Dependent claims 11-12** depend from independent claim 1 and are allowable by virtue of this dependency, as well as for additional features that they recite.

**Independent claims 18 and 31** were rejected for the same reasons as claim 1, and are allowable for reasons similar to those given above.

**Dependent claims 26-27** depend from independent claim 18 and are allowable by virtue of this dependency, as well as for additional features that they recite.

**Dependent claims 38-39** depend from independent claim 31 and are allowable by virtue of this dependency, as well as for additional features that they recite.

## CONCLUSION

For at least the foregoing reasons, claims 1-40 are in condition for allowance. Applicant respectfully requests reconsideration and withdrawal of the rejections and an early notice of allowance.

If any issue remains unresolved that would prevent allowance of this case, **Applicant requests that the Examiner contact the undersigned to resolve the issue**.

Respectfully Submitted,

Lee & Hayes, PLLC
Representatives for Applicant

/Dominic S. Lindauer/ Dated: 8/29/08
Dominic S. Lindauer (dominic@leehayes.com; x229)
Registration No. 61417
David Divine (daved@leehayes.com; x233)
Registration No. 51275
Customer No. 22801

Telephone: (509) 324-9256
Facsimile: (509) 323-8979
www.leehayes.com